

ABSTRACT

Embodiments of the invention reduce the probability of success of a DOS attack on a node receiving packets by decreasing the probability of random collisions of packets sent by a malicious user with those sent by honest users. The probability of random collisions may be reduced in one class of embodiments of the invention by supplementing the identification field of the IP header of each transmitted packet with at least one bit from another field of the header. The probability of random collisions may be reduced in another class of embodiments of the invention by ensuring that packets sent from a transmitting IPsec node to a receiving IPsec node are not fragmented.